PRIVACY ISSUES
IN TELECOMMUNICATIONS

PRIVACY ISSUES IN TELECOMMUNICATIONS

Susan Alter
Law and Government Division

Revised 24 January 1996

Library of Parliament
Bibliothèque du Parlement

Research Branch

The Research Branch of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Research Officers in the Branch are also available for personal consultation in their respective fields of expertise.

Available in Canada through
your local bookseller
or by mail from
Canada Communication Group -- Publishing
Ottawa, Canada K1A 0S9

Catalogue No. YM32-1/93-2-1996-01E
ISBN 0-660-16547-3

N.B. Any substantive changes in this publication which have been made since the preceding issue are indicated in **bold print.**

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRIVACY ISSUES IN TELECOMMUNICATIONS*

ISSUE DEFINITION

Telecommunications technology is developing at an unprecedented pace. Services that may once have seemed visionary are becoming commonplace. But with the arrival of many welcome innovations such as cellular phones, fax machines and "call display," has come a host of unwelcome threats to privacy. For example, scanners have penetrated intimate cellular phone conversations; miscued fax machines have delivered sensitive information into unsafe hands; and consumers have been driven to oppose surcharges levied for blocking "call display," arguing that their anonymity should not carry a price tag.

Some commentators feel that such privacy erosions are simply the cost that society must bear for the personal conveniences and economic benefits that technological progress makes possible. For privacy advocates such as the federal Privacy Commissioner, however, privacy is a non-renewable and diminishing resource, and every new technology-induced assault on privacy that is tolerated worsens our society's "technological trance," in which we permit technology to limit individuals' rights rather than letting such rights limit technology. The Ontario Privacy Commissioner has warned that the cumulative damage of numerous small invasions of privacy could far outstrip the apparent benefits. In addition, the federal Privacy Commissioner has noted that without a meaningful measure of privacy, our other fundamental freedoms of expression, belief and association risk being eroded as well.

Canadians are not oblivious to the threat that telecommunications and other technologies pose to their privacy, according to a national privacy study released in March 1993; moreover, they want something done about it. This Current Issue Review will survey particular privacy problems generated by new telecommunications technologies and discuss the approaches taken to address them.

---

* The original version of this Current Issue Review was published in October 1993; the paper has been regularly updated since that date.

BACKGROUND AND ANALYSIS

"Privacy" is a complex concept with negative as well as positive aspects. According to certain privacy experts, privacy is the right not to be disturbed (or the right to be left alone), the right not to be known (or the right to be anonymous), the right not to be monitored (or the right to intimacy), and the right not to have one's identifying information exploited (or the right to control one's personal information). Others have narrowed privacy down to two salient features: the right to be protected against intrusions and the right to control information about oneself and one's activities. No matter how one chooses to define privacy, as a right it clearly goes to the heart of preserving human dignity and autonomy.

In the telecommunications field, privacy issues have often surfaced on a case-by-case basis; that is, the introduction of a new technology or service, such as caller ID, has raised a new privacy concern. Solutions in these circumstances tend to be narrow, technical fixes that unfortunately can quickly be overtaken by new technological developments. As a result, the search for solutions has broadened to adopt a more general principle or policy-based approach. The federal government and the private sector have joined forces to develop privacy principles to guide the telecommunications industry and some key industry players have created privacy codes to guide the delivery of specific services. Both approaches, the technology-specific and the more generalized, will be examined in the pages that follow.

A. Technology-Specific Privacy Problems and Solutions

1. Telephone

a. Unsolicited Calls

Corporations make unsolicited phone calls for a variety of purposes -- to sell goods and services, to solicit donations, and to acquire information that may be used in future sales or fundraising campaigns. A majority of Canadians believe that uninvited calls from telemarketers are invasions of privacy; yet, many do not rank such calls among the most serious of such invasions,

according to two major surveys. *Privacy Revealed* reported in 1993 that 70% of respondents had received uninvited telephone calls in the previous month from someone selling a product or soliciting a donation. While 18% were "not at all concerned" about these intrusions, another 18% were "moderately concerned" and 29% were "extremely concerned." In comparison, over half the respondents were "extremely concerned" about informational privacy and the potential to link personal information held in different data banks. ***Surveying Boundaries: Canadians and their Personal Information*** **reported similar results in 1995.**

In the early 1990s, as the popularity of telephone soliciting increased in Canada, complaints from disgruntled subscribers to the Canadian Radio-television and Telecommunications Commission (CRTC) about unsolicited phone calls and faxes also increased exponentially. They rose from 355 in 1990 to 6,480 in 1993, when the CRTC was given new statutory authority to control unwanted calls pursuant to the new *Telecommunications Act*. Before that legislation was enacted, the CRTC regulated telecommunications pursuant to the *Railway Act*, which did not give it the express power to regulate unsolicited phone calls. As a result, it regulated certain types of unsolicited phone calls, such as those sent out by automatic dialling-announcing devices (or ADADs), by drawing on its general power to set the terms and conditions governing how telephone companies carry telephone traffic.

Newly armed with an express power to regulate unsolicited calls pursuant to the 1993 *Telecommunications Act*, mindful of the Act's objective "to contribute to the protection of the privacy of persons," and concerned about the sharp rise in complaints from the public about the failure to control these unwanted phone calls, the CRTC took steps in June 1994 to curb the commercial use of ADADs. In Telecom Decision CRTC 94-10, it banned the use of pre-recorded, computer-dialled telephone solicitations, including such calls placed by or on behalf of charities, and put conditions on their use for non-solicitation purposes.

No ban or restrictions were placed on the use of ADADs by police, fire departments, schools, hospitals and others, for public service functions such as conveying messages in emergency situations. Rules were, however, imposed on commercial uses of ADADs (that is other than for solicitation purposes) such as automated calls to collect overdue accounts, schedule

appointments, and conduct market research or opinion polls. These rules pertained to calling hours, identification of the caller, and call disconnection.

The purpose of the Commission's ban on ADAD solicitation was not to stop telephone solicitation as such, but to put an end to the automated format. It concluded that uninvited ADAD solicitations cause greater inconvenience or nuisance than live-voice calls, and, because they do not permit the called party to interact with the caller, are more likely to be perceived as an intrusion. The Commission predicted that, even if the courts were later to find that its ban violated the Charter's guarantee of freedom of expression, it would be allowed to stand as a reasonable limit demonstrably justified in a free and democratic society. The Commission's ADAD ban extends to all the carriers within its jurisdiction.

In the same decision, the CRTC announced some new rules applying to uninvited solicitations by live-voice and fax machine. The new rules were to apply in Bell Canada's operating territory to any calls selling or promoting a product or service, or soliciting money or money's worth from the party called, including calls made on behalf of charitable organizations. The most noteworthy is the "Do Not Call" rule, which requires parties soliciting business or money by live-voice calls or facsimile machine to respect a call-recipient's request not to be called again and to ensure that the person's name and telephone number are removed from the calling list. If a caller ignores such a request, the line used to make the unwanted solicitation will be shut down. **In June 1995, the CRTC approved similar rules regulating unsolicited live-voice calls made using AGT Limited's lines.**

b. Subscribers' Phone-listing Information

In March 1995, at the request of White Directory of Canada (White), the CRTC reversed a 1990 decision allowing telephone companies, such as Bell Canada, to refuse to provide their residential telephone directory database information in machine-readable (electronic) form to third parties for commercial exploitation. For those who opposed White's application to reverse the 1990 decision, the main concern was that the privacy of residential phone subscribers could be eroded; subscribers could be more exposed to unsolicited phone calls if their non-confidential

phone-listing information were readily accessible in electronic format to, for example, telemarketers. Consequently, in reversing its decision, the Commission introduced measures to ensure the protection of telephone customers' privacy. It required the phone companies to advise residential customers that they might ask to have their names and numbers "de-listed" (i.e., removed at no charge from any telephone-listing databases which can now be sold to third parties). Subsequently, White applied to the CRTC to reconsider the privacy protection created in allowing subscribers to opt for de-listing, but the Commission did not modify its position (Telecom Decision CRTC 95-14).

c. Call Management Services

Call Management Services (CMS) provide a number of features designed to enhance the privacy of telephone subscribers. One such feature is "call display," also referred to as caller ID, which displays the telephone number of an incoming call on the subscriber's phone. In May 1990, the CRTC approved Bell Canada's application to introduce CMS, including the call display feature, despite concerns expressed by some interveners. They had identified the possible ill effects of caller ID as including enabling an abusive partner to track down a spouse in hiding, jeopardizing the safety of police informants and undercover agents, and destroying the anonymity of persons calling government departments, businesses, distress lines and health information centres. In approving CMS, the CRTC attempted to balance the positive and negative effects of the call display feature by making call-blocking available to all subscribers at a nominal charge and free of charge to certified shelters for victims of domestic violence. This compromise did not suit many consumer and privacy advocates, who asked the CRTC to review its decision.

In 1992, the CRTC revisited the call display privacy issues and decided that all telephone subscribers, not just certain exempted customers, should be able to block the display of their phone numbers free of charge, by electing to do so when they place a call. This reconsideration of the caller ID debate was important in that it recognized that both aspects of

privacy, the right to know who is calling and the right to remain anonymous in placing a call, warrant reasonable protection.

In June 1994, the CRTC approved proposals by Bell Canada, AGT Limited and Maritime Telegraph & Telephone Limited to enhance their call display feature by adding the caller's name. The CRTC recognized that, as with the introduction of number display, the introduction of name display would raise important privacy concerns. As a result, it approved name display on condition that the companies provide certain privacy safeguards, including free per-call blocking or a permanent display of "private name" in lieu of the caller's name.

d. Call Interceptions

In 1974, intercepting or eavesdropping upon private telephone conversations was made an offence under the *Criminal Code*, thus recognizing such intrusions into privacy to be socially unacceptable. When Parliament created this offence, however, it also created some exceptions in order to balance the legitimate privacy interests of Canadians with society's needs for effective law enforcement. To assist police in criminal investigations, they were allowed to intercept a private phone call if they obtained a proper judicial authorization (e.g., a warrant) or if they had the consent of one of the participants in the private communication. The latter practice, called participant surveillance, was opposed in *R.* v. *Duarte* (Supreme Court of Canada 1990) as being an unreasonable search and seizure and thus violating section 8 of the *Canadian Charter of Rights and Freedoms*. The Supreme Court held that the interception of private communications by the police with the consent of one of the participants, but without obtaining prior judicial authorization, infringed the Charter. This and related electronic surveillance decisions rendered by the Court between 1990 and 1992 had a significant impact on certain types of police investigations. Undercover operations, in particular, became more dangerous because the Court's rulings knotted the electronic lifeline between undercover officers and their back-up teams. Legislation to revive some of the police's electronic surveillance practices in a manner more consistent with the Charter was introduced through Bill C-109, amending the *Criminal Code*, which was enacted by Parliament and came into force in August 1993. Essentially, the amendments generally allow participant

surveillance only with prior judicial authorization, but condone it without prior judicial authorization to prevent bodily harm to the consenting party.

The Supreme Court of Canada's 1990 decision in *R.* v. *Thompson* is also noteworthy in that it indicated that an authorization to tap pay phone conversations is not a *carte blanche* to do so indiscriminately; the privacy rights of third parties who are not suspects in the investigation must be respected. Therefore, the Court ruled that information gleaned by police from leaving tape recorders on automatic play overnight, without regard to whether a targeted suspect could reasonably be expected to use the tapped pay phone that night, constituted an unreasonable search and seizure.

Bill C-109, which amended the *Criminal Code* to set new parameters on participant surveillance, also amended the Code and the *Radiocommunication Act* to deal with the growing problem of intercepted calls from cellular and cordless phones. Since these phones actually broadcast private conversations over public airwaves, the conversations they transmit are not considered "private communications" as defined in the Code (unless they are encrypted) and are therefore not protected by the provision making the interception of "private communications" illegal. Bill C-109 did not outlaw the devices used to intercept cellular and cordless phone calls; rather, the bill made it an offence to intercept a radio-based telephone communication, such as a cellular phone call, maliciously or for gain, or to use or disclose information obtained from such interception. In addition to facing prosecution and a jail term for committing such an offence, an individual could also face a conviction and fine up to $25,000 or a civil action under amendments made simultaneously to the *Radiocommunication Act*. The result of these amendments is that, while eavesdropping on cellular and cordless phone conversations may not be prevented, it has become illegal and costly to disclose the contents of such conversations. Members of the Canadian Association of Journalists opposed these amendments, arguing that they constituted a "gag law." Others felt Bill C-109 did not go far enough to protect the privacy of radio-based communications.

The Information Highway Advisory Council, in its September 1995 report, added its voice to those claiming that when using radio-based telephones Canadians should have the same level of privacy protection under the law as they have when using wireline telephones. The Council recommended that the federal government amend the *Criminal Code* and the

Radiocommunication Act accordingly. The Council also recommended that, except as authorized by the responsible minister, the manufacture, importation, sale, distribution and modification of digital scanners capable of monitoring radio-based telephones, including cellular telephones, be prohibited. Finally, the Council recommended that government and industry cooperate to speed up the development and introduction of affordable encryption services for radio-based communications. **The federal government's response to the report is expected in March 1996.**

2. Facsimile Machines

a. Junk Faxes

The Better Business Bureau of Metropolitan Toronto estimated in June 1993 that as many as five million junk faxes were being sent out daily in Canada; this equated to 300 tonnes of paper a day and 1.5 million trees each year. The damage caused by junk faxes is not only environmental. Phone companies, the CRTC and consumer advocate groups have been besieged by complaints from victims of the deluge. Such victims include organizations who resent receiving unwanted fax transmissions on paper for which they have had to pay and lawyers whose efforts to close deals have been sabotaged because their office fax machines were tied up by uninvited advertising transmissions. Unsolicited faxes, like other unsolicited calls, are generally considered an invasion of privacy, since they arrive uninvited and often at inopportune times.

The CRTC decided in Telecom Decision 94-10, June 1994, that persons soliciting business or money via fax machines hooked up to Bell Canada lines should be required to adhere to some basic operating rules. Most importantly, they would have to respect the requests of other Bell Canada customers that no further unsolicited faxes be sent to them. Violators would risk having their fax lines shut down by Bell Canada.

Although these new rules applied only to Bell Canada's customers, similar rules have since been devised by other companies. For example, in late 1994 BCTel introduced, with the CRTC's consent, a "Do Not Call" rule for those sending unsolicited fax calls to its customers. Early in 1995, parallel rules were put in place to protect customers of AGT.

b. Fax Interceptions and Transmission Errors

Since fax machines transmit over telephone lines, fax transmissions can be tapped and intercepted by unauthorized persons; however, the major security risks associated with faxes are that the sender will dial the wrong fax number and thus send sensitive information to the wrong recipient, or that the faxed message, though directed to the right number, will be delivered to the wrong person. Unlike misdirected mail, which is received in a sealed envelope and can be returned unopened to the sender, a misdirected fax can be read by anyone. Given these pitfalls, the Ontario Information and Privacy Commissioner in 1989 developed comprehensive guidelines for Ontario government institutions on the security of fax transmissions and updated them in 1990. At the federal level, the Treasury Board has issued a brief policy statement regarding facsimile transmissions of classified and designated information. Federal institutions have, however, been left to develop their own specific procedures for faxing sensitive information. The policy is found in the *Security Volume* of the Treasury Board's *Information and Administrative Management Manual* and applies to such government institutions as departments, the RCMP, the Canadian Forces and CSIS.

3. Cable Television

Cable television services are undergoing a revolution as cable television is evolving from a one-way to a two-way interactive system that will allow viewers the freedom to select individually their entertainment and non-programming services (such as home shopping or banking). An addressable decoder or addressable box attached to the television set permits the cable company to release special programming or other services to the customer's home upon request. The cable industry hopes to provide an addressable box to every subscriber in Canada by the turn of the century.

But two-way cable television, in offering more personalized services, could also present a significant threat to the privacy of subscribers because it allows cable companies to accumulate, store and possibly distribute valuable information about subscribers' households. The cable companies' records of subscribers' viewing habits, tastes and service preferences constitute an

informational gold mine to which marketers likely would be eager to purchase access. Recognizing the potential privacy problems in the situation, the CRTC recommended in June 1993 that the Canadian Cable Television Association (CCTA) adopt privacy principles, or a code of fair information practices, for the cable industry. Such a code could, for example, include a provision prohibiting the sale of subscriber information without the subscriber's permission and, if the CRTC gave approval, adherence to the Code might even be incorporated into the terms and conditions of the cable companies' broadcasting licences.

Through the involvement of the Cable Television Standards Foundation, an independent body that oversees the implementation of the CCTA's *Cable Television Customer Service Standards*, the CCTA participated in the Canadian Standards Association (CSA) project to develop a model privacy protection code. Using the final version of this code as a base, the CCTA plans to draft a code that would apply specifically to the cable television sector.

4. Internet

Although the terms "Information Highway" and "Internet" are often used interchangeably, they do not describe exactly the same thing. The Internet makes up only part, albeit a significant part, of the information highway; stripped down to its fundamentals, the Internet is the world's largest computer network, say the authors of the *Canadian Internet Handbook*, Rick Broadhead and Jim Carroll. The Internet is created by linking computer networks worldwide via telecommunications systems. Computer users hooked up to the "Net" can trade any information that can be digitally reproduced – text, images or sound.

By contrast, the cable television-based component of the information highway is only at the developmental stage. Once they are more firmly in place, however, interactive cable television services could become a popular, alternative means of travelling the information highway.

The Internet is designed to improve knowledge, skills and communications on a world-wide scale, whereas the main purpose of interactive cable television will be to provide commercial services, such as home shopping, home banking and video on demand. Consequently, some interpreters of the information highway, such as Messrs Broadhead and Carroll, predict the development of *two* highways -- the "cerebral highway" of the Internet and the "couch-potato highway" of cable television. Whether the future delivers one, two, or more information highways, for the moment privacy problems occurring on the so-called "information highway" tend actually to result from using the Internet rather than from using interactive cable television services, simply because the Net is more pervasive.

Privacy is not a big concern for users of stand-alone computers. It is the ability of information to travel using computer networks linked by telecommunications lines that gives rise to many of the privacy concerns associated with the Internet. Some of these concerns are simply variations of those that arose with the use of earlier telecommunications technology; for example, unsolicited phones calls and fax messages have an Internet equivalent in the form of unsolicited bulk e-mail and Internet e-mail messages can be intercepted, just like telephone calls and fax messages.

In addition, the Internet produces brand new concerns; for instance, not only can e-mail messages be intercepted and recorded by outsiders, they also can be doctored or destroyed before they reach their destinations.

The greatest threat to individuals' privacy posed by the information highway, or more specifically by the linking of computers and databases in different locations, is the potential for making unauthorized use of personal information. The 1995 public opinion survey *Surveying Boundaries* found that 76% of respondents felt they had less control over their personal information than they had had ten years before. (In a 1992 privacy survey only 60% of respondents felt they had less personal privacy in their daily lives than they had had 10 years before.) At least some of this growing concern is attributable to computer technologies. The 1993 study *Privacy Revealed* found that 81% of respondents felt that

computers were reducing the level of privacy in Canada, with their most serious concerns being related to the linking of personal data held in the databases of different organizations. At least 89% of respondents were "moderately" to "extremely" concerned about such practices.

Privacy problems on the Internet are being solved through the development of rules for operating in cyberspace and through technological innovations such as encryption and firewalls. Encryption is electronic coding to protect the confidentiality of information as it travels over telecommunications systems. Firewalls are computers that prevent the millions of people using the Internet from gaining access to a company's or government's internal computer system. Firewalls serve as an institution's "security guards," standing between its private, internal databases and its door to the public domain of the Internet. Firewalls use passwords, keys alarms and other devices to fend off would-be intruders.

The conditions of service for customers linking to the Internet via AGT's Planet Service are an example of new operating rules being designed to protect privacy on the Net. Under a tariff approved by the CRTC in 1995, AGT is authorized to disconnect access to the Internet for any customer who sends an unsolicited mass distribution of any message in an intrusive manner to any other user or who acts so as to compromise the security of other computers on the Internet. Thus, customers who abuse bulk e-mail privileges or try to hack their way into private databases risk losing their lifeline to the Internet.

Dedicated privacy watchdogs believe that technological solutions and *ad hoc* rules will not suffice to ensure people's privacy on the information highway, since the greatest threat is the uncontrolled use of personal data. The federal Privacy Commissioner has been sounding alarm bells for many years and has concluded that the situation requires nothing short of legislation setting out broad minimum standards for the protection of personal information in the public and private sectors. More will be said about the push for a legislative solution in the next section of this paper.

B. General Privacy Protection Initiatives

In consultation and cooperation with industry, the federal government has been involved in several telecommunications privacy projects since 1992. For example, Consumer and Corporate Affairs, Statistics Canada, Communications Canada and the Privacy Commissioner of Canada collaborated with members of the private sector, including the Canadian Bankers' Association, Stentor Telecom Policy Inc., and Equifax Canada Inc., to sponsor *Privacy Revealed*, the comprehensive 1992 survey of Canadians' privacy concerns. The then Minister of Communications, Perrin Beatty, consulted with privacy advocates, telecommunications service providers, provincial governments and consumer groups in 1992 to produce the *Telecommunications Privacy Principles* and encouraged the private sector to set up a Telecommunications Privacy Protection Agency to enforce these principles. Also in 1992, the Canadian Standards Association organized a committee made up of volunteers from the public and private sectors to draft a model privacy protection code.

The federal government's approach to dealing with privacy issues in partnership with industry was supported by the respondents polled in *Privacy Revealed*. Of the people surveyed, 66% said the government should be working with business to come up with guidelines on privacy protection for the private sector. The survey also showed that the majority of people wanted to see active government involvement in privacy protection; 71% agreed that the government should pass legislation to protect personal privacy and that privacy rules should apply to both the government and business.

1. Industry Codes Versus Legislation

In 1984, Canada committed itself to adhering to the Organisation for Economic Development and Co-operation's *Guidelines on the Protection of Privacy and Transborder Information*. The federal government had already passed the *Privacy Act* in 1982 to bring its institutions' data protection practices in line with these OECD Guidelines; it now agreed to encourage private sector industries to develop and implement personal data protection codes (sometimes called "codes of fair information practices") based on the same principles.

The Guidelines set out basic principles for protecting personal information and individual privacy including the rules that, without the consent of the individual concerned, personal data should not be used for any purposes other than those for which it was originally collected and that an individual should have the right to see and, if necessary correct, his or her personal information records. The purpose of the Guidelines was to prevent disparities from developing among member countries in the laws and practices adopted to protect informational privacy. It was believed such discrepancies could hamper the free flow of personal data across borders and disrupt important sectors of the economy, such as banking and insurance.

Unfortunately, by 1992 few private sector industries in Canada had developed their own codes to protect personal data and ensure fair information practices. As a result, the Quebec government rejected voluntary protections and introduced Bill 68, An Act respecting the protection of personal information in the private sector. (The bill became law in 1993.)

It was the growing need for adequate privacy protections and the private sector's dearth of voluntarily produced codes that in 1992 moved the Canadian Standards Association (CSA) to organize a committee to draft a model privacy protection code reflecting the OECD Guidelines and from which more detailed sector-specific codes could then be developed. **While the CSA model code has been finalized, its intended purpose – to help stragglers develop their own voluntary codes – is being reconsidered. The model code has accomplished its primary objective impressively, by setting a minimum national standard for the protection of personal information that both data users and data subjects find acceptable. But, in light of recent developments at home and abroad, the voluntary approach to implementing the code no longer appears practical.**

In February 1995, the European Union adopted a *Directive on Data Protection* which sets out the rules for the protection of Europeans' personal data. Article 25 of the directive prohibits businesses in member countries from transferring personal data for processing to non-member countries that lack an adequate level of protection. With the exception of Quebec, Canada has no privacy laws protecting personal information held by the private sector. According to privacy experts, such as Colin Bennett and the federal Privacy

Commissioner, Quebec's new law will meet the EU standard but the voluntary, self-regulatory codes used in the rest of Canada will not; this could become a serious impediment for certain Canadian businesses.

Also, as more and more networks interconnect and the flow of personal information intensifies, the merely voluntary adoption of information protection measures appears out-of-date and dangerous. Sound statements of principle and good intentions cannot guarantee informational privacy when personal data are accessible through the Internet, Pharmanet, and a host of other public and private networks and databases. In addition, as the federal Privacy Commissioner pointed out in his 1994-95 Annual Report, "Voluntary codes not only deprive the public of legal protection, but may well deceive us into relying on a chimera."

With the growth in both threats to informational privacy posed by technology and in Canadians' concern over the vulnerability of their personal data, the Privacy Commissioner has been forced to reject the self-regulating, voluntary approach favoured by industry and the government since the 1980s. Instead, he has become a strong advocate of entrenching a minimum national standard of privacy protection in legislation that would be binding on all sectors. He suggests that, ultimately, the greatest contribution of the CSA model code may be to serve as the framework for such legislation, rather than simply as the prototype for voluntary codes.

The federal Privacy Commissioner's campaign for nation-wide privacy protection legislation governing the public and private sectors is gaining momentum. In September 1995, the Information Highway Advisory Council indicated that it strongly believes in the need for national legislation to establish fair information practices on the information highway, supported by effective independent oversight and enforcement mechanisms. Among other things, its report recommended that the federal government develop and implement a flexible legislative framework for privacy protection for both the public and private sectors under its jurisdiction; this framework would permit the customization of codes while requiring everyone to adopt at least the basic standard set out in the CSA model code. (The government's response to the report is expected in March 1996.)

In October 1995, the Canadian Direct Marketing Association (CDMA), once a strong proponent of voluntary codes and self-regulation, became the first industry group in Canada to call for national privacy legislation to govern the private sector. In particular, it suggested that the federal government enact a set of privacy principles and require each industry sector to develop its own code that would meet both its specific needs and the standards set by the legislation. The CDMA believes such legislation would allay the fears of Canadian consumers and force all businesses to apply fair information practices.

2. Telecommunications Privacy Principles

In 1992 the Minister of Communications launched a project to create privacy principles that would apply specifically to the telecommunications industry. Six basic principles were developed through a public consultation process. Published late in 1992, they were intended to provide a framework for policy development in the sector and to serve as a response to the EC's then draft Directive on data protection. Essentially, they require: (1) recognition that Canadians have a right to expect their personal privacy will be protected when using telecommunications services; (2) provision of adequate information about the privacy implications of telecommunications services so that Canadians can make informed choices; (3) restitution such that new services that erode privacy will include safeguards to restore the privacy status quo at no charge; (4) consent from individuals to collect, use and disclose their personal information obtained by telecommunications service providers; (5) protection for Canadians from unwanted, intrusive forms of telecommunications; and (6) periodic review of the methods of ensuring privacy in telecommunications.

In keeping with the objective of less government regulation, but with awareness that consumers have little faith in watchdogs without teeth, the method proposed for the implementation of the privacy principles was joint enforcement by industry and consumers. A body called the Telecommunications Privacy Protection Agency (TPPA) was to be established to accept, investigate and resolve telecommunications-related privacy complaints. The TPPA was to be funded by the

telecommunications industry and run by representatives of consumer groups, the industry and privacy experts. The actual establishment of the Agency has been in doubt since the election of a new federal government in October 1993.

3. CRTC

The CRTC is required by the *Telecommunications Act* (section 47) to exercise its powers and perform its duties with a view to implementing the Canadian telecommunications policy objectives, one of which is "to contribute to the protection of the privacy of persons." In addition, section 41 of the Act expressly authorizes the Commission to prohibit or regulate unsolicited telecommunications. Thus, the CRTC now has a strong legislative mandate to deal with privacy issues that arise in providing telecommunications services. Even before it had such a clear mandate, however, the CRTC did address privacy issues when it regulated telecommunications pursuant to the *Railway Act*. For example, it had issued decisions on automatic dialling announcing devices (ADADs), call management services (CMS), and phone companies' general terms of service, which were designed to include a provision protecting the confidentiality of customer information (Telecom Decision CRTC 86-7). In the past, the Commission dealt with privacy issues on a case-by-case basis, as specific issues arose. Since it was given newly defined responsibilities for privacy protection, the Commission has not become more proactive in setting out general privacy rules and guidelines for the telecommunications sector; it continues to deal with issues on a case-by-case basis.

PARLIAMENTARY ACTION

Specific legislative proposals and actions taken with respect to protecting privacy are summarized below.

A. Charter of Rights and International Commitments to Human Rights

Privacy is not a right, like freedom of expression, that is explicitly protected by the Charter from government interference. The Privacy Commissioner of Canada did appeal to the Special Joint Committee on a Renewed Canada in 1991 for an express right to privacy to be added to the Constitution, but such a right was not included in the constitutional amendments proposed by the unsuccessful Charlottetown Accord.

At present, a limited right to privacy is recognized in the Charter's section 8, which provides that everyone has the right to be secure against unreasonable search or seizure. In comparison, the Quebec government has entrenched a general right to personal privacy in section 5 of its *Charter of Human Rights and Freedoms*, which guarantees everyone the right to respect for his or her private life.

As a member of the United Nations, Canada subscribes to the basic standards of human rights set out in the *Universal Declaration of Human Rights* in 1948. Article 12 states that no one shall be subjected to arbitrary interference with his or her privacy and everyone has the fight to legal protection from such interference. This declaration is not legally binding and enforceable, but Canada acceded to the *International Covenant on Civil and Political Rights* in 1976 (article 17 of which restates the privacy rights set out in article 12 of the *Universal Declaration of Human Rights)*, which is binding and enforceable.

B. *Privacy Act*

The *Privacy Act* was adopted by Parliament and came into force in 1983 to protect the privacy of individuals by ensuring that their personal information held by government institutions would not be misused and by providing them with a right of access to this personal information. The Act in effect established a code of fair information practices for federal government institutions but it did not extend to the federally regulated private sector. The Standing Committee on Justice and the Solicitor General, in its 1987 report *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, recommended that the *Privacy Act* be amended so that its informational privacy protections would apply in the federally regulated private sector. Later in the

year, the Government of Canada tabled *Access and Privacy: The Steps Ahead*, its response to the Justice Committee's report. It promised the Act would be amended to extend to Crown corporations and that the government would work closely with provincial and territorial governments to promote the implementation of the OECD Guidelines in the public and private sectors; however, no indication was given that legislation affecting the federally regulated private sector would be forthcoming. In June 1993, Quebec became the first province to pass legislation protecting personal information in the private sector. This legislation includes provisions regulating telemarketers' use of "nominative lists" (lists of names, addresses or telephone numbers).

C. *Telecommunications Act*

New legislation regulating telecommunications in Canada, the *Telecommunications Act*, came into effect in October 1993. Section 7 of the Act incorporates a list of Canadian telecommunications policy objectives, the final one being "to contribute to the protection of the privacy of persons." The Act directs the CRTC, in section 47, to exercise its powers and perform its duties with a view to implementing these policy objectives, including the privacy protection objective. In addition, it gives Cabinet the authority, in section 8, to issue directions to the CRTC of general application concerning broad policy matters associated with the Act's telecommunications policy objectives, if Cabinet decides the Commission needs guidance in this respect. Finally, under section 41, respecting unsolicited telecommunications, the Act gives the CRTC the express authority to regulate the growing problems with unsolicited phone calls and junk faxes.

D. *Criminal Code*

In 1974, the *Criminal Code* was amended by the *Protection of Privacy Act*, which added a new Part related to "Invasion of Privacy." This included provisions prohibiting the interception of "private communications," such as wire-tapping phone conversations. In 1993, these provisions were extended by Bill C-109 to protect the privacy of cellular phone calls. Encrypted cellular phone signals are now included under the definition of "private

communications" and, like conventional phone calls, are protected from illegal interceptions. In addition, the new amendments make it illegal to intercept radio-based telephone communications maliciously or for gain. In tandem with the latter amendments, changes were made to the *Radiocommunication Act* to protect the privacy of cellular and other wireless or radio-based telephone communications.

E. *Radiocommunication Act*

In 1993, amendments to the *Radiocommunication Act* created the offence of unlawfully making use of or divulging a radio-based telephone conversation. The offence was accompanied by stiff penalties -- imprisonment up to one year and/or a fine up to $25,000 for an individual and up to $75,000 for an offending corporation.

CHRONOLOGY

1 September 1968 - The first detailed study of privacy protection in Canada was completed and released in a report by the Ontario Law Reform Commission. Among the 20 key areas of concern identified for further study was the need to establish controls over private sector acquisition, use and disclosure of personal information.

30 June 1974 - The *Protection of Privacy Act*, amending the *Criminal Code* and adding to it a new Part entitled *Invasion of Privacy*, came into force.

1 July 1983 - Parliament proclaimed the *Privacy Act*, which protects the privacy of Canadians with respect to personal information held by federal government institutions (but not information held by the federally regulated private sector).

29 June 1984 - The Government of Canada announced its formal adherence to the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*.

31 March 1987 - The House of Commons Standing Committee on Justice and the Solicitor General tabled a report entitled *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, which reviewed the

Privacy Act and recommended that its rules for protecting personal information be extended to the federally regulated private sector.

15 October 1987 - The government's response to *Open and Shut*, entitled *Access and Privacy: The Steps Ahead*, was tabled. It announced the government's intention to extend the *Privacy Act* to apply to Crown corporations and their wholly-owned subsidiaries.

9 December 1991 - Federal Privacy Commissioner Bruce Phillips recommended to the Senate-Commons Committee on a Renewed Canada that the right to privacy be entrenched in the Charter.

7 December 1992 - Federal Communications Minister Perrin Beatty issued the *Telecommunications Privacy Principles* and announced that a Telecommunications Privacy Protection Agency would be established to ensure their implementation.

29 March 1993 - The findings of an in-depth survey of Canadians' attitudes and concerns about privacy were made public in a report called *Privacy Revealed*.

15 June 1993 - Quebec's National Assembly passed Bill 68, An Act respecting the protection of personal information in the provincial private sector.

1 August 1993 - Bill C-109, amending the *Criminal Code* and *Radiocommunication Act* with respect to intercepting phone calls, came into force.

25 October 1993 - Bill C-62, An Act respecting telecommunications, came into force.

20 February 1995 - The European Union Council of Ministers adopted a Directive on Data Protection, which included a clause prohibiting the transfer of personal data for processing in non-member countries that lack adequate data protection laws.

SELECTED REFERENCES

Communications Canada. *Privacy Protection in Telecommunications - Discussion Paper and Proposed Principles*. Department of Communications Information Services, Ottawa, June 1992.

Communications Canada. *Telecommunications Privacy Principles*. Minister of Supply and Services Canada, Ottawa, December 1992.

CRTC. "Call Management Service - Blocking of Calling Number Identification." Telecom Decision CRTC 92-7, Ottawa, 4 May 1992.

CRTC. "Use of Telephone Company Facilities for the Provision of Unsolicited Telecommunications." Telecom Decision CRTC 94-10, Ottawa, 13 June 1994.

Graves, Frank, Nancy Porteous and Patrick Beauchamp. *Privacy Revealed - The Canadian Privacy Survey*. Ekos Research Associates Inc., Ottawa, March 1993.

Privacy Commissioner. *Annual Report Privacy Commissioner 1990-91*. The Privacy Commissioner of Canada, Ottawa, 1991.

Privacy Commissioner. *Annual Report Privacy Commissioner 1991-92*. The Privacy Commissioner of Canada, Ottawa, 1992.

Privacy Commissioner. *Annual Report Privacy Commissioner 1992-93*. The Privacy Commissioner of Canada, Ottawa, 1993.

Privacy Commissioner. *Annual Report Privacy Commissioner 1993-94*. The Privacy Commissioner of Canada, Ottawa, 1994.

Privacy Commissioner. *Annual Report Privacy Commissioner 1994-95*. The Privacy Commissioner of Canada, Ottawa, 1995.

Public Interest Advocacy Centre and Fédération nationale des associations de consommateurs du Québec. *Surveying Boundaries: Canadians and their Personal Information*. PIAC and FNACQ, Ottawa and Montreal, 1995.

CASES

R. v. *Duarte*, [1990] 1 S.C.R. 30.

R. v. *Thompson*, [1990] 2 S.C.R. 1111.

ACCO®

ACCOPRESS™MMC

YELLOW	25070	JAUNE
*BLACK	25071	NOIR*
*BLUE	25072	BLEU*
RL. BLUE	25073	RL. BLEU
*GREY	25074	GRIS*
GREEN	25075	VERT
RUST	25078	ROUILLE
EX RED	25079	ROUGE

ACCO CANADA INC.
WILLOWDALE, ONTARIO

* INDICATES 75% RECYCLED 25% POST-CONSUMER FIBRE

*SIGNIFIE 75 % FIBRES RECYCLÉES, 25 % DÉCHETS DE CONSOMMATION

BALANCE OF PRODUCTS 25% RECYCLED

AUTRES PRODUITS: 25 % FIBRES RECYCLÉES

ACCO® USA
WHEELING, ILLINOIS 60090
ITEM NO. 25074
0 50505 25074 5
LT. GRAY/GRIS/GRIS CLARO
MADE IN USA